AMENDMENTS TO THE CLAIMS

IN THE CLAIMS:

A complete set of claims is provided below.

Please amend Claims 13-16, 18-25 and 27-28 as indicated below.

1.-9. (Canceled)

10. (Withdrawn) An anti-alteration system for homepage, comprising:

a public-web-server computer retaining the safe-web-files encrypted from a usual web file which includes non-executable files and at a user browser side computer executable file;

a CGI Gateway module for sending a request information to a CGI Gateway means, wherein when said public-web-server computer gets said request information from a user browser to executes a CGI (Common Gateway Interface) program, said request information is a URL format including IP address, comment and parameters, however said public-web-server does not execute said CGI program before doing generation process, send said request information to said CGI Gateway module only; and

a send request information to original-web-server means, in which at said CGI Gateway module, said request information is modified automatically to a new request that is received by said original-web-server and sent to said original-web-server which comprises;

means for using said modified request information got from said CGI Gateway module, executing CGI program in said original-web-server computer,

means for sending a http header and CGI output contents from said CGI program to said CGI Gateway at said public-web-server computer; and

means for sending a CGI output from said CGI Gateway module to a user's browser passing through a public-web-server or directly.

11. (Withdrawn) An anti-alteration system for homepage, as recited in claim 10, wherein chaos encryption technology is used to do encryption/decryption.

12. (Withdrawn) An anti-alteration system for homepage, as recited in claim 10, wherein said real time check technique uses a message authentication technology using chaos theory.

13. (Currently Amended) An anti-alteration system for web-content, comprising:

a public-web-server ~~computer retaining~~ **configured to store** safe-web-files encrypted from ~~usual~~ original web-contents including one or more ~~kinds~~ **types** of static files and one or more ~~kinds~~ **types** of dynamic file, and ~~providing~~ **configured to provide** HTTP web server ~~functions.~~ **funtions;**

a private-web-server ~~computer which retains~~ **configured to store** said original ~~usual web-content~~ **web-content,** ~~and connects~~ said ~~public-web-server computer~~ **private-web-server provided to said public-web-server through** ~~though means for avoiding illegal access as well as through~~ a ~~firewall,~~ **firewall;**

~~means for authentication checking, decrypting and sending a safe-web-file,~~ wherein when a web visitor's request is received, said public-web-server ~~computer checks~~ **is configured to verify that** said safe-web-file ~~that if said safe-web-file is no illegally~~ **has not been improperly** altered, deleted or replaced, said public-web-server ~~computer sends back~~ **further configured to decrypt one or more of said safe-web-files and respond to said visitor** ~~said web-content decrypted from said safe-web-file to said web visitor with http or other protocol~~; and

~~a recoverable means for encrypting said web-content to create said safe-web-file on said private-web-server computer, wherein when said safe-web-file is illegally altered as checked by real_time_check technique on said public-web-server, said altered safe-web-file is automatically restored from said private-web-server~~ **said public-web-server further configured to automatically send a recovery request to said private-web-server when said public-web-server detects an unauthorized alteration of said safe-web-files, said private-web-server, in response to said recovery request, configured to create new safe-web-files by encrypting one or more files of said original-web-content and send said new safe-web-files to said public server through said firewall.**

14. (Currently Amended) The anti-alteration system, as recited in Claim 13, wherein said ~~**recoverable means incorporates with**~~ encryption comprises chaos encryption **technology to do encryption and decryption of said web-content for increasing the web server response speed and increasing security strong of whole system**.

15. (Currently Amended) The anti-alteration system, as recited in Claim 13, further comprising a ~~**real_time_check**~~ **real-time-check** module used on said public-web-server computer for linking to a decryption module ~~**of said authentication check means to said web server**~~, wherein said decryption module is ~~**able to be controlled by events of**~~ **configured to decrypt one or more of said safe-web-files in response to an HTTP** request received from said web visitor ~~**though http protocol**~~.

16. (Currently Amended) The anti-alteration system as recited in Claim 15, further comprising a real-time-check ~~**device which is able**~~ **module configured to** use ~~**a**~~ symmetric-key encryption to decrypt **one or more of** said ~~**safe-web-contents**~~ **safe-web-files** when said web visitor's request is received.

17. (Previously presented) The anti-alteration system, as recited in Claim 16, wherein said symmetric-key encryption is selected from a group consisting essentially of DES, 3DES and AES.

18. (Currently Amended) An anti-alteration system for web-content, comprising:

a public-web-server ~~**computer, employed**~~ **configured to store** ~~**with a prohibit web-content illegally alter function, retaining**~~ safe-web-contents that have been ~~**added**~~ **provided** with ~~**a prohibit illegally alter**~~ header information including a MAC (~~**Massage**~~ **Message** Authentication Code) generated ~~**by**~~ **from** said original web-content, and properties of **said** original-web-content including, name, size, date, and location thereof;

a private-web-server ~~**computer which retains**~~ **configured to store** said original web-content ~~**and connects**~~ said public-web-server ~~**computer which is added with said**~~

~~prohibit illegally alter function, though a means of avoiding illegal access as well as~~ **provided to said private-web-server** through a firewall;

~~a real_time_check technique, in which when a web visitor's request is received, separates a~~ **said private-web-server configured to separate said** header information ~~is separated~~ from a requested safe-web-file ~~which is added with an avoiding illegally alter header~~, and ~~at same time~~ using said MAC (Message Authentication Code) included in said header information to check ~~said safe-web-file by method of a message authentication technology~~ **an authenticity of said safe-web-file**;

~~separate header information, wherein said web visitor's request is received, said real-time check technique is used to check said safe-web-file and when said safe-web-file is checked being not altered, said header information from said safe-web-file is cut and the rest part is changed to said web content which is sent back from said public-web-server to said web visitor;~~ and

~~a recoverable means for adding~~ said **public-web-server configured to add new** header information to said original web-content to create a new safe-web-file on said private-web-server computer when an ~~illegally altering~~ **unauthorized alteration** of said safe-web-file is detected, wherein said new safe-web-file is sent to said public-web-server computer to automatically restore said **altered** safe-web-file ~~which is illegally altered~~.

19. (Currently Amended) The anti-alteration system, as recited in Claim 18, further comprising a ~~real_time_check~~ **real-time-check** module used on said public-web-server computer for linking to **an** authentication module ~~to said web server~~, wherein said authentication module is ~~able~~ **configured** to **provide authentication of said safe-web-file in response to a** ~~be controlled by events of~~ request received from said web visitor though http protocol.

20. (Currently Amended) The anti-alteration system, as recited in Claim 19, wherein said ~~real_time_check~~ **real -time-check** module uses a message authentication technology using chaos theory to check whether the safe-web-content ~~be~~ **has been** altered ~~or not~~.

21. (Currently Amended) The anti-alteration system, as recited in Claim 18, wherein said ~~real_time_check~~ **real-time-check** module that is ~~able~~ **configured** to link said ~~web server~~

public-web-server services ~~to any other~~ by using at least one message authentication technology selected from a group consisting essentially of MD4, MD5, and SHA~~-to find said web-content altered when said web visitor's request is received~~.

22. (Currently Amended) An anti-alteration system for web-content, comprising:

a public-web-server computer, ~~employed with a prohibit web-content illegally alter function, retaining~~ configured to store safe-web-files which have been encrypted from original web-contents and have been ~~added~~ provided with ~~a prohibit illegally alter~~ header information, said header information including a MAC (~~Massage~~ Message Authentication Code) generated from authentication checking said original web-content and properties including name, size, date, and storage location ~~on a hard disk~~ thereof;

a private-web-server computer which retains said original web-content and ~~connects said public-web-server computer which is added with prohibit illegally alter and decryption functions, though a means of avoiding illegally access as well as~~ which is provided to said public-web-server computer through a firewall;

a real-time-check ~~technique~~ module, in response to ~~wherein when~~ a web visitor's request ~~is received to obtain a requested for a~~ safe-web file, said real-time-check module configured to separate said ~~a~~ header information ~~is separated~~ from said safe-web-file ~~which is added with an avoiding illegally alter header,~~ and ~~at the same time~~ using a MAC (Message Authentication Code) included in said header information to ~~check~~ authenticate said safe-web-file by comparing said header information with ~~method of a message authentication technology;~~

separate header information~~, wherein when said web visitor's request is received, said real-time-check technique is used to check said safe-web-file and when said safe-web-file is checked being not illegally altered, said header information is cut from said safe-web-file and the rest part is decrypted to said web-content which is sent back from said public-web-server computer to said web visitor~~; and

a ~~recoverable means~~ recovery module, when an ~~illegally altering~~ unauthorized alteration of said safe-web-file is detected, said recovery module configured to ~~encrypting~~ encrypt said original web-content and ~~adding a~~ add header information to said original web-content to create a new safe-web-file on said private-web-server computer,

sending said new safe-web-file to said public-web-server computer to automatically restore said safe-web-file which has been altered.

23. (Currently Amended) The anti-alteration system, as recited in Claim 22, wherein said ~~recoverable means~~ recovery module ~~incorporates with~~ uses chaos encryption technology to do encryption and decryption ~~of said web-content for increasing the web server response speed and increasing security strong of whole system~~.

24. (Currently Amended) The anti-alteration system, as recited in Claim 22, ~~further comprising a real_time_check module used on said public-web-server computer for linking to decryption module and authentication module to web server, wherein said decryption module and authentication module is adapted to be controlled by events of request received from said web visitor though http protocol~~ **wherein said real-time-check module is configured to provide authentication of said safe-web-file in response to a request received from said web visitor through http protocol.**

25. (Currently Amended) The anti-alteration system, as recited in Claim 23, wherein said real-time-check ~~device is able~~ is configured to use a symmetric-key encryption to decrypt said safe-web-contents ~~when~~ in response to said web visitor's request ~~is received~~.

26. (Previously presented) The anti-alteration system, recited in Claim 25, wherein said symmetric-key encryption is selected from a group consisting essentially of DES, 3DES, RC4 and AES.

27. (Currently Amended) The anti-alteration system, as recited in Claim 24, wherein said ~~real_time_check~~ real -time-check module uses a message authentication technology using chaos theory to check whether the safe-web-content ~~be~~ has been altered ~~or not~~.

28. (Currently Amended) The anti-alteration system, as recited in Claim 24, wherein said ~~real_time_check~~ real-time-check module ~~that is able to link said web server to any other message authentication technology selected from a group consisting essentially of~~ uses at least

one of MD4, MD5, and SHA ~~to find said web-content altered when said web visitor's request is received~~ for message authentication.